

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America

v.

ADESH BISsoon

Case No. 1:20-mj-599

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 2018 through Aug. 11, 2020, in the county of Hamilton in the  
Southern District of Ohio, the defendant(s) violated:

Code Section

18 U.S.C. 1349

Offense Description

Conspiracy to Commit Mail Fraud

This criminal complaint is based on these facts:

See attached affidavit of TIGTA Special Agent Sean Williams.

☒ Continued on the attached sheet.



Complainant's signature

Sean Williams, Special Agent, TIGTA

Printed name and title

Attested to by the Applicant in accordance with Fed. R. Crim. P. 4.1.

Date: 8/12/2020



Judge's signature

City and state: Cincinnati, Ohio

Hon. Karen L. Litkovitz, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO**

**IN THE MATTER OF THE CRIMINAL  
COMPLAINT OF:**

**ADESH BISSOON**

)  
)  
)  
)  
)

**Case No.** 1:20-mj-599

**AFFIDAVIT IN SUPPORT OF  
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Sean Williams, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I submit this affidavit in support of a criminal complaint and arrest warrant against ADESH BISSOON for a violation of 18 U.S.C. § 1349 (Conspiracy to Commit Mail Fraud).

2. I am a special agent with the U.S. Department of the Treasury, Treasury Inspector General for Tax Administration (“TIGTA”). TIGTA is tasked with ensuring the integrity of the IRS and its infrastructure security and protecting the IRS against external attempts to corrupt tax administration. TIGTA special agents are certified criminal investigators with authority to carry firearms, make arrests, execute warrants, and administer oaths. I am assigned as a Criminal Investigator within the Cincinnati Field Office. I am also a member of TIGTA’s Cyber Investigative Cadre, whose mission is focused on communications- and computer network-related investigations. I have been employed by TIGTA since 2018. Prior to my employment with TIGTA, I was a special agent, investigator, and police officer with multiple U.S. federal government agencies. I have received training from the National Cyber-Forensics and Training Alliance and TIGTA’s Cybercrimes

Investigative Division.

3. The facts in this Affidavit are based on my personal knowledge as well as on information I learned from other sources, including law enforcement databases, reports prepared by other law enforcement officers, and conversations I have had with other law enforcement officers and witnesses involved in this investigation.

4. Because I am submitting this affidavit for the limited purpose of securing a criminal complaint and arrest warrant, I have not included every fact that I know about this investigation; I have set forth only those facts that I believe are necessary to establish probable cause to believe that BISSOON has violated 18 U.S.C. § 1349.

**PROBABLE CAUSE**

**A. The government is investigating an identity-theft and mail-fraud scheme in which the subjects have exchanged stolen PII and fraudulent identity documents.**

5. TIGTA is investigating an identity-theft and mail-fraud scheme in which victims' stolen PII has been shared among multiple subjects, including via email and text.

6. In 2019, email search warrants showed that, starting in at least November 2013 and continuing through late 2019, ADESH BISSOON, Coconspirator 1, and Coconspirator 2 sent and received emails containing many individuals' personally identifiable information ("PII") and/or fraudulent identity documents, including fraudulent driver's licenses and Social Security cards. Some of the individuals whose PII was exchanged among the coconspirators had addresses in the Southern District of Ohio.

7. In connection with the scheme, as I describe below, the coconspirators caused physical checks, drawn from an account in the name of a victim, to be mailed to a P.O. Box in

Cincinnati for deposit into a financial account controlled by BISSOON.

**B. Evidence suggests that the user of ABissoon26@gmail.com is BISSOON.**

8. From at least November 2013 through December 2019, ABissoon26@gmail.com exchanged PII and fraudulent identity documents with KeyStone11@gmail.com, an account used by Coconspirator 1. For example, on October 18, 2014, KeyStone11@gmail.com sent ABissoon26@gmail.com an email titled “GAME PLAN” that contained lists of victims’ names and bank account numbers and this message: “try ur best to be extremely cautious...be a strategic method to keep all accounts active....the grand total for everyone combined for both TX & WA is about \$720,000. So let me know if ur GAME...”

9. I believe BISSOON is the user of ABissoon26@gmail.com. First, the email signature lists “ADESH BISSOON.” Second, on the phone of Coconspirator 2—at whose house agents found evidence of identity theft (such as debit cards, personal checks, and bank account statements in other people’s names) during a January 2020 search warrant—agents found messages with phone number XXX-XXX-5027 (the “5027 Phone”), dated October 2019 through January 2020, for which the contact name was “ADESH.” The 5027 Phone was activated in BISSOON’s name in February 2005, and credit cards in his name were used to pay the bill from 2015 through May 2020. Third, ABissoon26@gmail.com contained a photo of a scanned copy of a Florida driver’s license with BISSOON’s name and birthdate from May 2019; a “selfie” appearing to show BISSOON with his driver’s license from February 2015; and a scan of BISSOON’s passport from January 2015. Finally, as discussed below, logins via an IP address subscribed to BISSOON link him to the account.

**C. Evidence suggests that BISSOON is also the user of JerryLaster403@yahoo.com.**

10. From November 2016 to November 2019, Coconspirator 2's email accounts exchanged suspected stolen PII and fraudulent identity documents with JerryLaster403@yahoo.com. In May 2019, JerryLaster403@yahoo.com also received an email from an account used by Coconspirator 1 that contained credit reports, a driver's license, and a Social Security card for a suspected victim.

11. JerryLaster403@yahoo.com contains evidence that BISSOON uses it. For example, I found an altered utility bill from March 2016 (sent in January 2017) and an hourly invoice template from January 2019; the metadata showed that both were authored by "ADESH BISSOON." I also found an email from BeenVerified.com, a company that provides criminal-background and people-search services. Information from BeenVerified.com showed that in July 2017 the account opened by JerryLaster403@yahoo.com ran a search on the 5027 Phone (BISSOON's number) and "ADESH ALVIN BISSOON" (BISSOON's full name).

**D. J.A. is likely a victim of the scheme under investigation.**

12. In ABissoon26@gmail.com, I found an Excel sheet, which the metadata show was authored in April 2012 by BISSOON, that contained a table that I believe BISSOON created to help him remember the bank accounts he had opened in other people's names. For example, the table included an entry for victim Jerry Laster and an associated bank account. Another entry listed J.A.'s name and six associated bank accounts. On this particular spreadsheet, there were eight names of suspected victims; in total, I have found approximately

a dozen such spreadsheets, which BISSOON sent to KeystoneInc11@gmail.com from October 2014 through January 2015.

13. During my review of JerryLaster403@yahoo.com, I found an email dated July 9, 2019, to an account used by Coconspirator 2 with subject line “Suggested schedule to create paper for players.” Based on my knowledge of this investigation, I believe that the coconspirators use the term “paper” to refer to fraudulent documents; I have seen several communications in which the coconspirators appeared to be using the term “paper” in that way. The email listed the name of a suspected victim for each day of the week. J.A.’s name was listed for “Wednesday.” BISSOON wrote to the recipient: “I suggest to hit for one player per day.”

14. In January 2016, an email account used by Coconspirator 2 received an email from “[nameredacted]225@gmail.com” (incorporating J.A.’s full name). The attachment, which metadata show BISSOON wrote, was titled “JA Info for DL and SS.docx”; it said in part “Use this address for the utility bill.” The address was 1508 Bay Road Apt. 729 in Miami Beach, a building in the Flamingo Point complex, a complex in which BISSOON resides at least part time, as explained below. Later the same day, Coconspirator 2 sent back a driver’s license in J.A.’s name that listed the Bay Road address.

**E. Coconspirator 2 and BISSOON communicated about suspected identity fraud via text as recently as January 2020.**

15. Text communications in October 2019 between BISSOON (using the 5027 Phone) and Coconspirator 2 also revealed screenshots of what I believe was an attempted mobile deposit for \$950.53 by BISSOON into a bank account in the name of F.K. I believe

that F.K. is a victim of the scheme, because I know from reviewing emails from FIUKid30@gmail.com that F.K.'s name was contained in multiple lists of PII sent to or received by Coconspirator 2. On October 31, 2019, BISSOON texted Coconspirator 2 a screenshot from the bank account showing that the check had been returned unpaid because the bank believed it was altered and/or fictitious.

16. As of January 2020, when Coconspirator 2's phone was seized, the last communication via text between Coconspirator 2 and BISSOON was on January 7, 2020. Coconspirator 2 wrote, "Sent the paper to my friend Jason. He at the office working hard. Lol." BISSOON responded, "I will contact you soon with the requested information." Based on my knowledge of this investigation, I believe that, when Coconspirator 2 referred to "the paper," he meant falsified documents created using stolen PII; I have seen several communications in which, based on context, I believe Coconspirator 2 and his co-conspirators were using the term "paper" in that way.

**F. Checks in the name of suspected victim J.K. and in the name of an LLC in J.K.'s name were mailed to Cincinnati, Ohio, for deposit into an account in BISSOON's name.**

17. In September 2017, J.K. reported to the Miami-Dade Police Department in Florida that someone had opened financial accounts in his/her name without authorization. I believe that J.K. is a victim of the scheme under investigation, because evidence from BeenVerified.com shows that an account associated with JerryLaster403@yahoo.com (an account used by BISSOON, as described above) received a data report containing J.K.'s PII. Additionally, my review of JerryLaster403@yahoo.com revealed that it contained a purported

Social Security card in J.K.'s name; based on my training and experience and knowledge of this investigation, including other evidence that the coconspirators have a template for a Social Security card, which they have used to create Social Security cards in various victims' names, I believe that the purported Social Security card in J.K.'s name was created by the coconspirators in furtherance of the fraud.

18. Between approximately March 16 and April 6, 2018, physical checks in the name of J.K. or in the name of "[J.] K Consulting LLC" were mailed, via an online bill-pay service that creates and mails physical checks, to a P.O. Box for Fidelity Investments located in Cincinnati, Ohio, for deposit into an account in BISSOON's name. These checks totaled more than approximately \$9,500.

19. From approximately June 4 through June 22, 2018, that same Fidelity Investments account in BISSOON's name received several mobile deposits from a bank account in the name of J.K. These deposits totaled more than \$50,000. Fidelity Investments later identified these deposits as "altered/fictitious"; however, by the time the bank had made that determination, the money had been transferred out of BISSOON's account. The bank then closed BISSOON's account for suspected fraud.

**G. Evidence suggests that BISSOON has lived at a certain address on Bay Road in Miami Beach, Florida, since April 2018.**

20. As explained below, I believe that BISSOON has lived at a certain apartment within the "Flamingo Point" complex in Miami Beach (the "Miami Beach Apartment") at least part time since April 2018.

21. When I reviewed the contents of ABissoon26@gmail.com, I found that on



April 12, 2018, the user sent an email to “Melissa.capo@aimco.com (Flamingo South Beach – Center Tower)” with the subject line “C 2302 Move In Inspection Results.” 2302 is the apartment number for the Miami Beach Apartment. The body of the email contained what appear to be the results of the tenant’s move-in inspection for apartment C 2302 at the Flamingo Center Tower. Based on my knowledge of the layout of Flamingo Point, I believe that the “C” in the apartment number (“C 2302”) refers to the fact that the Miami Beach Apartment is in the complex’s center tower.

22. From April 2018 through January 2020 (the latest date for which I have search warrant results), Amazon.com sent email receipts to ABissoon26@gmail.com listing the shipping address as the Miami Beach Apartment.

23. In April 2018, Atlantic Broadband IP-11 was registered to BISSOON, with the 5027 Phone as the associated phone number, at the Miami Beach Apartment. On May 1 and July 9, 2019, IP-11 was used to log into ABissoon26@gmail.com (which address, as noted, has been used in furtherance of the fraud). As of June 8, 2020, the account was still active at the Miami Beach Apartment.

24. Evidence from the IRS shows that the coconspirators have opened LLCs using victims’ PII; many were registered in 2017 and 2018 to various apartments at 1508 Bay Rd., Miami Beach, FL—the address of the neighboring tower at Flamingo Point (which complex contains the Miami Beach Apartment). BISSOON received mail at 1508 Bay Rd. Apt. 509, and he opened an internet service account for 1508 Bay Rd. Apt. 521, before moving to the Miami Beach Apartment.

25. In 2016, four PayPal accounts were opened under JerryLaster403@yahoo.com,

victim J.L.'s name, the business name "Laster Medical," and BISSOON's former address: 1508 Bay Road, Apt. 509. PayPal closed three of the accounts on May 10, 2016, for suspected fraud.

26. In April 2016, an American Express card was opened in J.L.'s name. The account is still active. As of July 2020, an address associated with the account was the Miami Beach Apartment.

27. In 2016, an account with PublicData.com, a website that allows users to obtain individuals' PII, was registered to JerryLaster403@yahoo.com at 1508 Bay Road. The method of payment was the American Express card in J.L.'s name registered to the Miami Beach Apartment. In 2016 and 2017, the account performed 339 searches, including searches for several individuals who have reported being victims of identity theft. The account was active through November 2019.

28. JerryLaster403@yahoo.com contained emails from January and March 2019 showing orders for two duplicate driver's licenses, one of which was for victim J.V. The shipping address was the Miami Beach Apartment.

**H. In August 2020, agents executed a search warrant at the Miami Beach Apartment and found evidence of the identity-theft and mail-fraud scheme, including credit and/or debit cards in victim J.K.'s name.**

29. On August 11, 2020, agents executed a search warrant at the Miami Beach Apartment. BISSOON was present.

30. During the search of the premises, agents found approximately 20 driver's licenses in the names of other individuals. Agents also found approximately 200 credit and/or debit cards and more than 20 checkbooks in other individuals' names.

31. At least seven of the credit and/or debit cards agents located at the Miami Beach Apartment were in the name of J.K., the victim described above in whose name physical checks were mailed to the Fidelity Investments P.O. Box in Cincinnati, Ohio. Another approximately four credit/debit cards found on the premises were in the name of “[J.] K Consulting LLC” (with “[J.]” being victim J.K.’s first name).

32. Based on my training and experience and knowledge of this investigation, I believe that most or all of individuals whose names appear on the driver’s licenses and credit/debit cards found in BISSOON’s residence are victims of the identity-theft and mail-fraud scheme described in this affidavit.

33. During an interview, BISSOON admitted to agents that he had attempted to deposit fraudulent checks from accounts in other individuals’ names. When agents asked how often he had successfully deposited such checks, BISSOON claimed that it had not worked often and that he had had “terrible luck.” When agents asked BISSOON about the Fidelity Investments account in his name that had received funds via physical checks mailed to a Cincinnati P.O. Box and in the name of J.K. or “[J.] K Consulting LLC,” BISSOON admitted that his account had been closed due to fraud.

//

//

//

//

//

//

**CONCLUSION**

34. Based on the foregoing, I respectfully request that the Court issue the proposed criminal complaint and arrest warrant.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Sean Williams', written over a horizontal line.

Sean Williams  
Special Agent - Treasury Inspector General for  
Tax Administration (TIGTA)

Attested to by the Applicant in accordance with Fed. R. Crim. P. 4.1 on August 12,  
2020.

A handwritten signature in blue ink, appearing to read 'Karen L. Litkovitz', written over a horizontal line.

HON. KAREN L. LITKOVITZ

United States Magistrate Judge